Running Head: HOME-BASED HEALTH INFORMATION WORKER

Information Privacy and Security for the Home-based Health Information Worker

Monica S. Dunnehoo

East Carolina University

In partial fulfillment of the requirements for DTEC 6823

Dr. Phil Lunsford

November 29, 2005

Abstract

As the health care industry adopts and implements more information technology and embraces “remote” employees and contractors, a computer literate workforce educated in utilizing confidential patient data is needed. Telecommuters and independent contractors in the fields of medical coding, billing, and transcription need to be cognizant of federal legislation regarding health information privacy, security, and the relevant safeguards required to protect the confidential patient data in their possession. This report offers guidance on implementing Health Insurance Portability and Accountability Act of 1996 (HIPAA) regulations and other privacy and security rules as they apply to the home-based health information worker. Common sense coupled with computer literacy and a wealth of free information available on the Internet are factors for success.

Many people dream of a career that provides a flexible work schedule and the opportunity to work at home using their computers. Medical transcription, medical coding, and medical billing are three health information careers that have been marketed and promoted as "work at home" opportunities, enabling the individual to balance home, work, and family. Before outlining recommended information security practices and procedures for those interested in these at-home opportunities, several key terms and principles must be clarified to establish a baseline vocabulary in health care, security, and privacy.

TRENDS IN TELECOMMUTING

The home-based health information worker is a broad term coined to describe individuals in a variety of employment situations related to health care. As the name implies, some or all of this work may be done "off-site" at a satellite location, usually the individual's primary residence.

"Telework," "virtual work," "mobile work," or as it is more commonly called "telecommuting" means that employees have shifted their work location from their employer's place of business to a home office; the employee's presence at the office is not required every day in order to fulfill work obligations. The employer may or may not provide computer equipment, technical support, and Internet service for these home workers.

There is conflicting data on the percentage of Americans who did some work at home as part of their primary job. The 2005 survey from ITAC (formally known as the Telework Advisory Group of WorldatWork) reports that 45.1 million (33 percent) of

135.4 million American workers are working in a variety of locations outside of their employer's office (2005). This is in contrast with data from the Bureau of Labor Statistics, which reports that 20.7 million (15 percent) of the 136,602 nonagricultural workers reported in May 2004 that they worked at home at least once per week (2005).

The National Institute for Standards and Technology (NIST), a federal agency that works with industry to develop and apply technology, measurements, and standards, recommends several strategies for a successful telecommuting program in a "cook book" format. Among other things, it recommends that telecommuters sign an agreement outlining the terms and conditions for telecommuting and that the employee's supervisor endorse it to ensure proper authorization for remote access. Because of varying technical computer skills, "whenever practical, agencies should provide telecommuting users with systems containing pre-configured security software and necessary hardware" (Kuhn, Tracy, & Frankel, 2002). The American Health Information Management Association (AHIMA) has suggestions for content to include in the telecommuting policy available in its public online library (Dougherty & Scichilone, 2002).

Regardless of the employment arrangements, working at home is not without its own risks. *NIST SP 800-46: Survey for Telecommuting and Broadband Communications* proposes that the very successes in protecting government and corporation computing resources have made telecommuters, and by association home-based health information workers, targets for "malicious entities." However,

> "While there will always be risks associated with remote access to an organization's resources, most of these risks can be mitigated through careful planning and implementation" (Kuhn, Tracy, & Frankel, 2002).

So who are these “malicious entities.” Per research reported by the University of Arizona, Tucson, amateur hackers are “by far the biggest threat on the Internet at the current time,” responsible for about 90% of all hacking activity (2004). The thoughtful employer or home-based business owner must weigh the risks and benefits of telecommuting and remote access and make informed decisions to minimize and mitigate these risks based on information available at the time.

HOME-BASED EMPLOYMENT IN HEALTH INFORMATION

Whether serving as a medical transcriptionist (MT), a medical coder, or medical biller, the efforts of these professionals ensure that doctors and other health care workers have accurate information about patients. These positions are viewed by the medical community as distinct skill sets with different career paths.

Various professional organizations offer seated exams for members to demonstrate competence in their fields. These certifications are voluntary and are geared to the experienced worker (Rowell & Green, 2004). Research shows that those with national certifications, in particular coding certificates, do earn higher wages than non-certified coders (AAPC, 2004).

So what do MTs do? As experts in the language of medicine “with keen listening skills and fast typing ability, these transcriptionists use their training to document medical histories…they turn health care providers’ spoken notes into well-edited, typed reports” (Shniper, 2001). These recorded dictations were traditionally recorded on audiocassettes, but with developments in technology, other means to store these recordings digitally have been developed. Regardless of the media used to capture the spoken word and the delivry

method to the MT, once these reports have been proofed, edited, and signed, they become part of the patient's medical record, which is a legal document (Rowell & Green, 2004).

The industry itself is not new. According to Molly Malone, executive director the Medical Transcription Industry Alliance (MTIA) in an interview with AHIMA, "The first large contracts with transcript companies were signed around 1959…thousands of "cottage industry" medical transcriptions were started…today, nearly half of transcription is outsourced to specialized vendors" (Rhodes, Dennis & Roach, 2004).

The U.S. Department of Labor Bureau of Labor Statistics' *Occupational Employment and Wage Estimates November 2004 Report* states that approximately 94,000 people were employed as medical transcriptionists with a median hourly wage of $13.76 or $28,630 annually. Of those, more than 88% were employed by hospitals, physicians, and outpatient care centers. Note that these estimates do not include self-employed workers (2005).

The other desired at-home positions include medical coding and medical billing. Unfortunately for statistical purposes, the Bureau of Labor Statistics lumps these two positions into the general category "Medical Records and Health Information Technicians" for reporting purposes while in reality they are two very different occupations. Approximately 160,000 people are employed in medical records with a median hourly rate of $12.55 and annual salary of $26,110. More than 67% were employed by hospitals, physicians, and outpatient care centers; nursing homes, and federal government were other major employers. As with MTs, these estimates do not include self-employed workers (Bureau of Labor, 2005).

Medical coders or coding specialists carefully review the patient's medical record to identify the diagnoses that were treated and the services that were provided during the treatment session. After "abstracting" the data, they then translate these complex diagnoses and procedures into codes that can be processed by insurance companies for reimbursement.

This profession requires a firm command of medical terminology, anatomy and physiology, critical reading and thinking skills, and a knowledge of coding conventions as one can see from the following example. The medical record states "patient was treated for excision of a 1-cm skin lesion on her arm. The pathology diagnosis was benign nevus." Using the appropriate coding manuals, the coder translates the diagnosis and service provided into codes, specifically 709.9 representing the benign nevus (which is a mole) and 11401 representing the removal of the lesion (Rowell & Green, 2004).

A unique challenge for the home-based medical coder is that the original medical record should never leave the medical facility. Making and transporting paper copies is problematic, but with the advent of online electronic medical records that allows remote access to the abstracting systems and clinical systems, "remote coding" is expected to grow as a profession. AHIMA estimates that nearly 5,000 coders now work from remote locations (Shearer, 2001).

Medical billers or medical billing clerks/specialists compile and maintain records related to the services and materials provided by the facility from documents called "superbills" or "encounter forms." Billers use specialized computer software to enter the charges, patient and insurance payments, and adjustments to the patient accounting records, and prints bills. Other responsibilities include handling follow-up questions

from patients and resolving payment discrepancies or errors with insurance companies and other third-party payers. Attention to detail, bookkeeping skills, and ability to work well under pressure are needed (MHA Health Career Center, 2004).

With NCR (carbonless) superbills, it is possible for the home-based biller to transport and bring work home. If remote access to the practice's network is not available, methods to manually synchronize the home and office computer must be developed and rigidly followed so that data is not corrupted or damaged during the transfer.

The Mississippi Hospital Association (MHA) Health Career Center analyzed the employment opportunities for these three fields. It estimates that the average annual salary for medical coding specialists is $28,500; for medical transcriptionists, $27,900; and for medical billing clerks, $26,600. It reports the future is "outstanding" for medical coding specialists because of the increased scrutiny over medical records by the government and insurance companies and "excellent" for MTs as medical records are transformed into electronic medical records (EMRs). The future is not so bright for medical billers, however. It projects a modest growth for this position, but at the same time, states that with improvements in computer technology, fewer billers will be needed (2004).

COVERED ENTITIES, BUSINESS ASSOCIATES, AND HIPAA

The home-based health information workers identified previously may work for covered entities, for business associates of covered entities, or subcontract with business associates and/or covered entities. But what do these

terms mean? A covered entity is a health plan, health care provider, or other facility that transmits any health information in electronic form in connection with a HIPAA transaction. HIPAA, which stands for Health Insurance Portability and Accountability Act of 1996, is a far-reaching piece of federal legislature whose requirements will be discussed in more detail later in this report.

To continue, a HIPAA transaction is "the exchange of information between two parties to carry out financial or administrative activities related to health care" (Krager & Krager, 2005). Examples of these electronic health information transactions include claims creation and processing, enrollment and eligibility, payment and remittance advice, eligibility, health plan premium payments, and coordination of benefits (CMS, 2003).

A business associate is basically a subcontractor or vendor for the covered entity. What distinguishes the business associate from other vendors or trading partners is that the business associate has the potential to need or gain access to confidential patient information. While business associates are individuals or companies that perform some kind of service on behalf of a covered entity, the business associate is not part of the covered entity's workforce (CMS, 2005).

Many people may be under the impression that information privacy and security are new "hot buttons" for the health care industry. In fact, the medical industry has long established traditions regarding privacy, confidentiality, and security of patient information. Sensitive and confidential data is routinely shared between the patient, health care provider, insurance company (sometimes called a "third-party payer"), and by extension, to the employees, subcontractors, and vendors of those providers and payers.

As a matter of contract law, health care providers cannot release patient information to insurance companies or other agencies unless the patient signs a release of medical information form. To quote Rowell and Green,

> "Privacy is the right of individuals to keep their information from being disclosed to others. Once information is disclosed (e.g., for the purpose of obtaining health care), it is essential that confidentiality of the information be maintained. Confidentiality involves restricting patient information access to those with proper authorization and maintaining the security of patient information. Security involves the safekeeping of patient information (2004).

If common sense and tradition alone were not enough to dictate the prudence of protecting confidential health information in one's possession, the U.S. Congress has enacted a variety of laws to protect health information from threats to security, integrity, and unauthorized use. To this end, the home-based health information worker must have a solid knowledge and understanding of a key piece of federal legislation, commonly known by its acronym "HIPAA."

Title I of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) protects health insurance coverage for workers and their families when they change or lose their jobs. Title II of HIPAA sets forth administrative simplification standards that "will improve the efficiency and effectiveness of the nation's health care system by encouraging the widespread use of electronic data interchange in health care" (CMS, 2005). This includes the security, privacy, and standards for electronic submissions and exchange of health care information, otherwise known as the "HIPAA triangle" (Fadlalla, A. & Wickramasinghe, N., 2004). There are three other titles to HIPAA, but they are unrelated to information or security (Hash, Bowen, Johnson, Smith, & Steinberg, 2005).

HIPAA ELECTRONIC TRANSACTIONS AND CODE SETS

Standards for Electronic Transactions & Code Sets were to be implemented by October 16, 2003. Simply put, this means that the Centers for Medicare and Medicaid Services (CMS), which administers the federal health insurance program known as Medicare, requires the electronic submission of Medicare claim forms. To standardize the code sets used to record diagnoses treated and services provided by health care providers on claim forms, three publications are designated for use.

These publications are as follows: the *International Classification of Diseases, 9th Revision, Clinical Modification (ICD-9-CM), Volumes 1 & 2* to code diagnoses in both inpatient and outpatient settings; *Current Procedural Terminology-4 (CPT-4)* for outpatient services and encounters; *Health Care Common Procedure Coding System (HCPCS)* used for items, supplies, and non-physician services not covered under CPT-4; and *ICD-9-CM, Volume 3* for inpatient procedures (CMS, 2003).

HIPAA PRIVACY AND SECURITY

With the exchange of electronic data comes the need to maintain both the privacy and security of this confidential and sensitive health data. Title II addresses these concerns with separate privacy and security rules and oversight of same. The Office of Civil Rights (OCR), a division of the U.S. Department of Health and Human Services (HHS), oversees and enforces the Privacy Rule while CMS, also an agency under HHS, is responsible for implementing “various unrelated provisions of the HIPAA security rules” (CMS, 2004).

The HIPAA Privacy Rule (45 CFR, Parts 160 and 164) protects all "individually identifiable health information" and calls this "protected health information" or PHI. The Privacy Rule contains provisions for when this PHI may be used and disclosed by certain groups; in addition, it directs that policies and procedures be enacted to reasonably limit uses and disclosures of PHI to the "minimum necessary." Its deadline for implementation was April 14, 2003. Most readers will recall being requested by a variety of health care providers (physicians, pharmacists, and dentist to name a few) to sign "Privacy Practices Notices," one of the Privacy Rule requirements from a few years ago.

The HIPAA Security Rule (45 CFR, Parts 160, 162, and 164) applies to PHI when it is in electronic form (EPHI) only. EPHI may be transmitted over the Internet, stored on a computer hard drive or network, a CD, a disk, audiotape, videotape, or other related means. The Security Rule does not cover PHI that is transmitted or stored on paper or provided orally; it is electronic only.

To reiterate, the Privacy Rule sets the standards for who may have access to PHI while the Security Rule sets the standards for ensuring that only those who should have access to EPHI will actually have access. The deadline for compliance of the Security Rule was April 21, 2005, for most health care organizations; April 21, 2006, is the deadline for small health care providers. A small provider is defined as "those with fewer than 25 full-time equivalent employees or a physician, practitioner, facility or supplier (other than a provider of services) with fewer than 10 full-time equivalent employees" (CMS, 2004).

To further clarify, all PHI, no matter whether electronic, oral, paper, or film, must be protected and kept private. This applies to PHI maintained or transmitted

electronically in connection with certain administrative and financial transactions. PHI includes demographic data, such as a person's name, address, date of birth, social security number, medical record number, insurance number, and other common identifiers. In addition, PHI refers to (1) the individual's past, present or future physical or mental health or condition; (2) the provision of health care to the individual; (3) the past, present, or future payment for the individual's health care; and (4) that which identifies the individual or for which there is a reasonable basis to believe the individual can be identified or recognized by this PHI (OCR, 2003).

While many health care providers, facilities, and payers have been concerned about the implementation of these federal regulations, it is important to note that

> "Reasonable safeguards do not require doing everything that is technically possible regardless of cost…the privacy regulations are scalable; small organizations are not expected to spend the same resources on privacy as large ones" (Lo, B., Dornbrand, L., & Dubler, N., 2005).

The HIPAA Security Rule applies the "CIA triangle" of confidentiality, integrity, and availability of information to electronic protected health information (EPHI). Whitman and Mattord defines the CIA triangle as follows:

> "Confidentiality of information ensures that only those with sufficient privileges and a demonstrated need may access certain information …Integrity is the quality or state of being whole, complete, and uncorrupted…Availability is the characteristic of information that enables user access to information without interference or obstruction and in a useable format" (2004, pp. 6-7).

CMS in its *HIPAA Information Series 1* (commonly called "HIPAA Security 101") applies these concepts to EPHI as follows: Confidentiality -- EPHI is accessible only by authorized people and processes. Integrity -- EPHI not altered or destroyed in an

unauthorized manner. Availability -- EPHI that can be accessed as needed by an authorized person (2004).

These security standards as defined in the Federal Register are developed to protect EPHI from unauthorized access, alteration, deletion, and transmission. While the Security Rule does not require specific technology solutions and is vendor neutral, reasonable and appropriate security measures must be implemented and documented. These standards are grouped into the following five categories: (1) administrative safeguards, (2) physical safeguards, (3) technical safeguards, (4) organizational requirements, and (5) policies and procedures and documentation requirements (2003, p. 8376). CMS notes that the Administrative Safeguards comprise over half of the HIPAA security requirements" (Federal Register, 2003).

The final Security Rule covers electronic protected health information (EPHI), but some security standards are either "required" or "addressable" which has led to some confusion regarding implementation. If a standard is required, then covered entities must implement the standard per the specification. If a standard is addressable, the covered entity determines if the specification is reasonable in its unique environment, documents the results of the assessment, and implements the specification if it is reasonable and appropriate for that covered entity (Hash, Bowen, Johnson, Smith, & Steinberg, 2005).

CMS warns that addressable does not mean optional. The Security Rule requires that a covered entity document the rationale for many of its security decisions and to keep these records for six years. In addition, CMS notes that "security is not a one-time project, but rather an on-going, dynamic process that will create new challenges as

covered entities' organizations and technologies change" (2004). One should note that any state law that is more restrictive than HIPAA takes precedence (AAMT, 2003).

It should not go without saying that a wealth of free information regarding HIPAA privacy and security is available on the Internet from government agencies like OCR, CMS, Workgroup for Electronic Data Interchange and Strategic National Implementation Process (WEDI SNIP) Security and Privacy Workgroup, as well as professional and trade organizations like AHIMA, American Association for Medical Transcription (AAMT), and the Healthcare Information and Management Systems Society (HIMSS). In particular, *NIST Special Publication 800-66: An Introductory Resource Guide For Implementing The Health Insurance Portability And Accountability Act (HIPAA) Security Rule* will prove particularly helpful.

CONSEQUENCES OF NONCOMPLIANCE WITH HIPAA REQUIREMENTS

Failure to comply with HIPAA can result in civil and criminal penalties per federal law, 42 USC § 1320d-5. In June 2005, the U.S. Department of Justice (DOJ) clarified that covered entities and other specified individuals could be held criminally liable under HIPAA and devised a three-tiered penalty scheme. If convicted of a misdemeanor, the penalty is a fine of not more than $50,000 and/or imprisonment for not more than one year. For violations committed under false pretenses, a maximum penalty of a $100,000 fine and/or five-year imprisonment can be imposed. For those offenses committed "with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm" the statute's highest penalties, fine of not more than $250,000 and/or imprisonment of not more than ten years, are possible (DOJ, 2005).

BEING HIPAA COMPLIANT

With civil and criminal penalties possible, Carole Gilbert of the American Association of Medical Transcription (AAMT) asked the question, "Who is going to tell us if we are doing this right?" She researched and determined that "no one can certify anyone else as being compliant" (2005). There have been so many misleading and unfounded marketing claims on this issue that the Office of Civil Rights cautions:

> "In fact, HHS and OCR do not endorse any private consultants' or education providers' seminars, materials or systems, and do not certify any persons or products as 'HIPAA compliant.' The Privacy Rule does not require attendance at any specific seminars. All of OCR's materials are available free on our web site" (OCR, 2003).

The confusion regarding "HIPAA compliant" may come from the data transaction testing requirement, which does mandate that all covered entities test HIPAA compliant software and systems for electronic claims submission (Frazier, 2003). These new standards relate only to receiving and exchanging electronic health information, specifically for insurance claims processing. (WEDI SNIP, 2002).

BUSINESS ASSOCIATE AGREEMENT

HIPAA administrative standards require a covered entity and its business associates to have a written contract or other arrangement because business associates may use PMI as they perform services for the covered entity (CMS, 2005). L. Gostin in the *Journal of the American Medical Association* notes that

> "…HIPAA does not authorize HHS directly to regulate the use and redisclosure of health information by the business associates of health care providers, such as lawyers, accountants, billing companies, and other contractors. Instead, the rule imposes a duty on covered entities to obtain satisfactory assurances that business associates will comply with privacy standards. If the covered entity knows of a violation and takes no steps to

> correct it, that entity can be held responsible for violation of the rules" (2001).

A covered entity's contract or other written arrangement with its business associate must contain the elements specified at 45 CFR 164.504(e). To summarize, the business associate agreement should include assurances that the business associate (1) will not use or disclose PHI other than for those purposes permitted by the agreement or by law; (2) will use appropriate safeguards to protect the confidentiality of the information; (3) report any use or disclosure not permitted by the agreement to the covered entity; and (4) implement records retention and destruction policies consistent with industry standards (OCR, 2004).

Fortunately, there are many free publications from reputable sources available on the Internet for this purpose. The WEDI SNIP Security and Privacy Workgroup outlines items to include in a typical business associate agreement. While this white paper is directed to MTs, it is readily applicable to other industries (2003). The AAMT has a free business associate agreement template specifically for MTs at its web site, but this template could be modified as needed for other professions (2003).

AHIMA's "Practice Brief on Letters of Agreement/Contracts" provides guidance on elements to include in a variety of written agreements; this brief also specifically references passages from the HIPAA privacy rule to include in business associate agreements (Rhodes & Hughes, 2003). In addition, the Office of Civil Rights has a sample business associate agreement available free of charge on its web site. The OCR notes, however, that "reliance on this sample is not sufficient for compliance with State law and does not replace consultation with a lawyer or negotiations between the parties to the contract" (2004).

Covered entities who have off-site or telecommuting employees are responsible for ensuring that all necessary security practices are in place and that privacy and security rules are being followed in these remote sites. Business associate contracts are not required in this situation, but confidentially agreements are well advised (WEDI SNIP, 2003).

While a subcontractor of a business associate is not technically a business associate of the covered entity, all MT subcontractors, freelance coders, or billers should be required to contractually agree to keep the same HIPAA restrictions when performing their duties using PMI. AHIMA and AAMT encourage covered entities to find out if their business associates subcontract out work and perhaps contractually forbid this practice if good faith measures cannot be taken to protect PMI. They believe that difficulties can arise when the business associate subcontracts out work without the knowledge of the covered entity (AAMT, 2003; Rhodes, Dennis, & Roach, 2003). Another preventive measure would be to conduct appropriate background checks on employees and businesses associates (Davis, Lemery, & Roberts, 2005).

PRACTICAL ADMINISTRATIVE, PHYSICAL, AND TECHNICAL SAFEGUARDS

The Security Rule FAQs acknowledge that remodeling an office or buying a new computer system can be prohibitively expensive, particularly for a small practice (Lo, Dornbrand, & Dubler, 2005). By extension, the “reasonable” standard for small health care providers should be transferable to administrative, physical, and technical safeguards for the home office, so home offices will not have to be remodeled, etc.

Another problem facing covered entities and business associates who subcontract to third parties is the lack of sophistication and/or training by business associates and their subcontractors so that they can be knowledgeable of HIPAA privacy and security. HIPAA horror stories include driving off with medical records on top of a car or leaving transcription tapes and other materials on the front porch for people to pick up and drop off in baskets are not unheard of (ASIHealth.com, 2005). One of the most famous incidents happened in October 2003 when a Pakistani subcontractor, in a dispute with a medical transcription company over payment, threatened to release patient information on the web. (Davino, 2004).

With these HIPAA horror stories as a backdrop, let's look at some common-sense accommodations the home-based health information worker can immediately make to be compliant with HIPAA's administrative, physical, and technical safeguards. The following are compiled from various sources, including *HIPAA for MTs* available from the AAMT.

(1) Do not work in a public area of the home; the kitchen or dining room table will not provide the minimum visual and physical security needed when working. (2) Have your computer and file cabinets in a lockable room; of course, don't leave the key in locations where it can be used by unauthorized people. (3) A "clean desk" policy at the end of the work shift will ensure that PHI is not available to family members, house guests, or others who may gain access to your locked home office. (4) Make sure your computer monitor does not face the door or window, even if it's on a second floor. (5) If you need to leave your workstation for a break, log off the computer; do not rely on screen saver to hide your on-screen data. (6) If using a courier service, be sure this

company is bonded. (7) Whether using a courier or delivering/picking up materials yourself, place these items in an opaque, secure, tamper-proof container. (8) When delivering work to clients, do not leave it unattended at the receptionist desk, etc. Have an employee of the practice sign and date that the materials were delivered properly. (9) If using a wireless phone, make sure it is digital, not analog, so that conversations cannot be picked up by outside parties. (10) Try not to discuss confidential matters within earshot of windows or doors. A neighbor could be outside gardening and overhear private conversations.

BEST PRACTICES

ASTM (originally known as the American Society for Testing and Materials), in cooperation with AAMT and MTIA members, has developed several standards and specifications for health care documentation. While *ASTM E1902-02: Standard Specification for Management of the Confidentiality and Security of Dictation, Transcription, and Transcribed Health Records* is specifically targeted to the medical transcription industry, it can readily be adapted for use by other home-based health information specialties for the creation of security best practices (ASTM, 2002; Hurley, 2004).

For the record, ASTM's E31.22 subcommittee on health information transcription and documentation was formed in 1995 with the mission "to develop standards for the systems, processes, and management of medical transcription and its integration with other modalities of report generation" (Gilbert, 2004). With the continued cooperation of

ASTM, AAMT, and MTIA, additional best practices for the health care industry will be documented in the future.

RECORDS RETENTION

The HIPAA Security Rule found in the Federal Register states that

> "Data backup need not result in increased access to that data. Backups should be stored in a secure location with controlled access. The appropriate secure location and access control will vary, based upon the security needs of the covered entity. For example, a procedure as simple as locking backup diskettes in a safe place and restricting who has access to the key may be suitable for one entity, whereas another may need to store backed-up information off-site in a secure computer facility" (2003, p. 8344).

HIPAA does not require covered entities to tape or digitally record oral communications, nor retain digitally or tape recorded information after transcription (HHS, 2003). Along this same line of reasoning, ASTM Standard E1902-02 recommends that transcription be stored or retained by the MT only for the length of time needed to complete the work. If at all possible, the home-based health information worker should not agree to keep copies of reports after completion for the covered entity or other party; the burden for record retention should be placed on the owner of the medical records. All data, whether paper or electronic, must be "carefully destroyed, erased, or deleted in a manner that prevents recovery by unauthorized persons" (ASTM, 2002). While both HIPAA and FACTA (Fair and Accurate Credit Transactions Act of 2003) legislate proper records destruction of personally identifiable information, neither provides specific standards for doing so (Hospitals for a Healthy Environment, 2003; FTC, 2004).

PAPER RECORDS DISPOSAL

Not everyone can accurately proof a manuscript simply by reading the computer screen; a hard copy printout provides a fresh tableau to view, mark, and correct. Should the home-based health information worker find it necessary to make hard copies for proofing or other reasons, these documents must be disposed of in a manner that protects the privacy of patients and, at the same time, does not allow for recovery or reconstruction of the data by third parties (ASTM, 2002).

Disposing of documents or other items in opaque trash bags is inadequate as these things could be recovered by "dumpster diving." This practice is not expressly illegal in the United States as all rights of privacy and ownership are forfeited by trash disposal 486 U.S. 35 (1988; Docket Number: 86-684). The U.S. Supreme Court (California v. Greenwood, decided May 16, 1988) underscored this fact with biting clarity: "It is common knowledge that plastic garbage bags left along a public street are readily accessible to animals, children, scavengers, snoops, and other members of the public."

Per Hospitals for a Healthy Environment (H2E), burning, shredding, pulping, and pulverizing are acceptable methods for paper destruction (2003). So which of these methods is advisable for the home-based health information worker? In *Medical Economics*, Perry concludes that "shredding is an excellent way to dispose of patient paperwork" (2004).

Now the decision becomes: Shred on-site or off-site? Most home-based health information workers would not find it cost-effective to contract with off-site or mobile on-site shredding services. The small volume, the need to purchase locked bins to secure PHI in the home office, and the documentation requirements to receive and maintain

certificates of destruction from these vendors and possible BA agreements would soon outstrip any advantages and go beyond the need to provide reasonable levels of safeguards to protect privacy (H2E, 2003).

Shredding on site is more practical and cost effective, but what type of shredder and level of security is needed? An internet vendor, ABCOffice.com, suggests that "the more important the document, the more important it is to use a shredder that will shred the documents into very small pieces" (2005). Shredders are available in strip cut, crosscut (confetti style), and top security cut versions. Top security meets DOD (Department of Defense) standards and offers the highest level of security, while cross-cut shredders are able to provide more security to shredded documents than a strip-cut shredder (Kahles, 1991). The volume of documents to be shredded and speed of shredding should also be purchase considerations.

ELECTRONIC MEDIA DISPOSAL

In addition to the destruction of paper records, electronic media destruction policies and procedures also need to be addressed. H2E states that methods selected for destruction and disposal should destroy data permanently and irreversibly (2003). Computer forensics specialists are not the only ones who have an impressive arsenal of methods for recovering deleted, encrypted, or damaged files to reveal information stored in a computer – so do hackers. Simply deleting a file on a computer or removable media does not destroy the data; it only deletes the file name from the file allocation table.

Data recovery software or services are available from third parties if one accidentally erases a needed file. The data recovery software reconstructs the link to the

deleted file to enable data recovery. Magnetic degaussing will leave the sectors in random patterns with no preference to orientation, rendering previous data unrecoverable (H2E, 2003); however, this is no guarantee that the appropriate kind of degausser is employed or that it is used properly to sanitize drives or other media (Connor, 2005).

Methods for destroying/disposing of diskettes include reformatting, pulverizing or breaking, and magnetic degaussing. Audiotapes or videotapes can be recycled by taping over them or pulverizing. Disks used in "write once-read many" (WORM) document imaging cannot be altered or reused, making pulverization an appropriate means of destruction/disposal (H2E, 2003).

PROTECTING THE HOME COMPUTER

All home-based health information workers should be expected to be knowledgeable about basic computer operation and maintenance, and it is just as important to be diligent and familiar with computer security technologies. As the Windows family of operating systems commands roughly 90 percent of the market and approximately 74 percent of computer owners use Internet Explorer as their web browser, this report will not discuss strategies specifically meant for Mac or Linux users, although many of the guiding principles of sound computing policy will be applicable for those users (W3Schools, 2005).

US-CERT (United States Computer Emergency Readiness Team) outlines a nine-step action plan to protect computers from common problems. The basic tasks are (1) install and use anti-virus programs; (2) keep the system patched, i.e., keep the operating system and web browser up-to-date with current updates and patches; (3) use care when reading

email with attachments; (4) install and use a firewall program, which acts like a security guard determining what does and does not gain access to the computer; (5) make backups of important files and folders; (6) use “strong” passwords; and (7) use care when downloading and installing programs. The two more advanced steps are (8) install and use a hardware firewall and (9) install and use a file encryption program and access controls. It goes on to say that “if financial resources are limited, they are better spent purchasing a commercial anti-virus program than anything else described in this guide” (2005).

In addition to the above security checklist, the NIST recommends (1) installing spyware removal tools and then updating and running these monthly; (2) securing wireless networks with an eight-step plan it documents in *NIST Special Publication 800-46*; (3) ensuring that appropriate encryption software, such as PGP or Norton Internet Security, is being used; (4) disabling file and printer sharing while online, particularly when accessing the Internet using cable modems, digital subscriber lines (DSL), or other high-speed connections; and (5) conducting an online security assessment for all major vulnerabilities (Kuhn, Tracy, & Frankel, 2002).

According to the NIST, one online scanning service found that more than 95 percent of the machines scanned have one or more possible vulnerabilities. Several commercial, online security assessment products are available from security experts McAfee and Norton; however, the NIST specifically recommends installing Microsoft Baseline Security Analyzer (MBSA), a tool that identifies common security misconfigurations and other vulnerabilities of Windows systems. MBSA is available for

free download at http://www.microsoft.com/technet/security/tools/mbsahome.mspx if desired (Kuhn, Tracy, & Frankel, 2002).

Note that some sections of the aforementioned *NIST SP 800-46* assume a background knowledge of various other aspects of networking and information security. "Less technical readers may find *NIST SP 800-41, Guidelines on Firewalls and Firewall Policy, January 2002,* a useful starting point for network security topics and then go on to read this publication" (Kuhn, Tracy, & Frankel, 2002). In addition, the University of Arizona, Tuscon has an excellent web site on information security and privacy written in a very casual, easy to absorb style, including instructions on how to determine if the sharing function in Windows is disabled for the type of operating system used (2003).

If Windows XP is the operating system employed, ensure that Microsoft Windows XP Service Pack 2 is installed with its new security and privacy enhancements. Per Microsoft, Windows XP SP2 has better safeguards to protect computers from hackers, viruses, and other online threats (2005).

PREVENTING UNAUTHORIZED ACCESS

At a minimum, all safeguards required for office workstations must also be applied to workstations located off site (CMS, 2005).To prevent unauthorized access, a simple five-step plan can be employed: (1) never share login ids and/or passwords. If any one else does need access to your computer, establish login IDs that limit file access; (2) use strong passwords, that is a password or passphrase that is not easily guessed. In general, a strong password needs to be 8+ characters in length and is a combination of upper and lower case text, numbers, and symbols (#, %, etc.). Of course, do not use

words found in the dictionary; (3) protect your security codes and passwords; don't write them down and leave them in plain site. Lock them up in a file cabinet if the user has difficulty remembering passwords; (4) always change the password provided by a vendor or other system provider; and (5) change your password frequently, every three to six months is recommended. Also, don't "recycle" passwords; once you've used it, discard it, and don't use it again (University of Arizona, Tuscon, 2004 & University of Texas at Austin, 2004).

Now let us look at some other tasks that the computer literate, home-based health information worker can do to secure her workstation.

USER ACCOUNTS AND PROFILES

Just as you have keys for file cabinets and locks on doors to secure physical files and folders in your home office, you can also limit access to your computer by administering local user accounts and using access control lists (ACLs). Per Whitman and Mattord,

> "ACLS regulate…who can use the system, what authorized users can access, when authorized users can access the system, where authorized users can access the system from, and how authorized users can access the system…(ACLs) restrict what users can access–for example, which printers, files, communications, and applications (can be used)" (2005, p. 123).

Operating system security has two goals: (1) to secure the system's hardware and software resources from improper use; and (2) to secure users' data from improper access. As such, the ability to assign different user permission rights is a valuable asset in theWindows XP operating environment. By setting yourself up with the Administrator

account, you can control adding hardware, modifying user accounts, changing access permissions, and installing software among, other things (Andrews, 2003, pp. 410-416).

As we all have mental lapses when it comes to passwords, it may be a good idea to utilize the "Forgotten Password Wizard" to create a forgotten password floppy disk that can be used if the user forgets her password. This wizard is accessed from the Control Panel, User Accounts. After selecting the desired user account, locate the Related Tasks panel near the upper left of the window; choose prevent a forgotten password and proceed from there. Andrews cautions that "this forgotten password floppy disk should be kept in a protected place so that others cannot use it to gain unauthorized access to the computer" (2003).

Mackey recommends that the Guest account be permanently disabled "as it offers a security exposure for servers on the network by providing an open door to Windows information for unauthorized users." In addition, the "real" Administrator account should be renamed with an "insignificant" name, one that does not indicate its true status. Mackey recommends crafting a decoy account named "Administrator" with very limited access privileges to lure hackers to the impotent account (2003).

For assets to which access cannot be sufficiently limited, you need to encrypt them strongly enough so that the time it takes to decrypt them is longer than their useful life.

DATA PRESERVATION AND BACKUP

"The three most common causes of total data loss are operating system failure, mechanical malfunctions of the hard drive, or failure in the software that controls the

hard drive" (Whitehead, 2005). These threats can be mitigated by observing established computing policies for storage and backup. Just like storing important papers in a fireproof safe at home or in a safety deposit box at the bank, the well-prepared computer user has on- and off-site storage for critical files in case of theft or natural disaster and has established regular backup schedules to preserve critical files.

While ASTM does not recommend permanent storage or retention of transcription materials (2002), the prudent home-based health information worker may desire to have "temporary" and/or off-site backups of works in process. Using removable media or Internet backup does have its inherent risks and benefits, however, which are discussed below.

Tape backup, floppy disks, and Zip disks are no longer the recommended backup media for the home office. Besides being slow and cumbersome, these media are becoming obsolete technologies; the marketplace has left them behind (Byers, 2003 & Fohl, 2005). Today, CD-Rs can hold up to 800 megabytes of data, while DVD-Rs can hold up to 4,700 megabytes. Old 3.5 inch floppies could only hold 1.4 megabytes (Byers, 2003).

Burning a CD or DVD or using an external hard drive or USB keychain/thumb drive is relatively quick, easy, and generally speaking, inexpensive according to James Martin of *PC World* (2005). He recommends (1) protecting critical files by backing them up every business day; (2) shopping around for secure file sharing; (3) mirroring , that is making a duplicate, of your hard drive with a portable external hard drive and online storage; and (4) keeping backup discs off-site in case of theft and natural diasters. While

these are good, sound recommendations for most computer users, they need to be modified when working with protected health information.

As Internet connection speed and capacity have increased for home users, so has the popularity of online backup. Also known as Internet backup or remote backup, this service is best for users making small backups of files. These service providers provide a limited amount of space on their web servers for a fee. Users are then allowed to upload and download files as needed from any location that has access to the Internet, eliminating the worry of backing up files on traditional physical media (Fohl, 2005). Per Whitehead (2005), online backups offer several advantages, including disaster recovery from this off-site storage and 128-bit level (military grade) encrypted data, making it effectively impossible for any one to intercept or decrypt the data as it is transferred across the Internet.

The security of the online data storage facility becomes one concern. Whitehead reassures that

> "These are invariably class-A facilities equipped with fire suppression, security cameras, personnel access controls, backup electricity generators, using multiple ISPs, high-end firewalls, and clustering and mirroring techniques to ensure the stored data is always available to clients. Except in exceptional cases, the storage premises will be more secure that the client's own premises" (2005).

OTHER NECESSARY COMPUTER SKILLS

Before making any changes to a computer system, such as downloading updates and patches or installing new software, a wise computer user will make it a habit to always create a "restore point" before making these changes. System Restore takes a "snapshot" of the system at a given point in time. Should software updates cause

unforeseen complications or malfunctions, System Restore can be used to return the computer back to its configuration prior to the restore point.

Note that System Restore does not affect user data on the hard drive, but any installation or configurations changes made after the restore point are lost, which is hopefully a good thing when downloads go bad (Andrews, 2003). Consult the built-in Windows Help and Support function for how to create and use restore points. Fohl notes that if the system has a virus or spyware, using System Restore will reverse the damage, but the virus/spyware is still lurking on your hard drive. In order to prevent the system from being compromised again, anti-virus and/or sypware removal tools must be used (2005).

If the computer malfunctions after updating drivers, locate “How to Roll Back to the Previous Version of a Device Driver” from the Windows Help and Support Center. Driver Roll Back reinstalls the driver used previously and restores any driver settings that were changed when the new driver was added; note, however, that it cannot restore printer drivers (Andrews, 2003).

Important skills for the computer literate home-based information worker to learn, but that time does not permit this report to cover, include (1) how to create an MS-DOS startup disk that can be used to boot into MS-DOS in an emergency; (2) how to start in Safe mode when Windows is “misbehaving”; (3) how to create an Automated System Recovery disk set of installation in case of hard drive errors or crashes; and most importantly, (4) learn how to help yourself by learning how to use the Windows Help and Support Center and the Windows Knowledge Base to seek out new information and assistance 24 hours a day, 7 days per week.

SUMMARY

In conclusion, employment opportunities for “remote” coding and medical transcription are improving. Employers are allowing more employees to telecommute and opportunities for home-based transcription, coding, and billing are increasing. An understanding of the HIPAA Privacy and Security Rules, coupled with common sense, computer literacy, and the wealth of free, yet reputable resources on the Internet will allow the prepared home-based health information worker to succeed.

References

ABCOffice.com (2005). Paper shredder guide. Retrieved on November 24, 2005, from http://www.abcoffice.com/shredder_guide.htm

AISHealth.com. (2005). HIPAA Compliance Strategies: When It Comes to Business Associates And Your PHI, Ignorance Isn't Bliss. (Reprinted from the August 2005 issue of *Report on Patient Privacy*). Retrieved on November 25, 2005, from *http://www.aishealth.com/Compliance/Hipaa/RPP_Business_PHI_Ignorance_Bliss.html*

American Academy of Professional Coders (2004, September). Certification wins the earning race. Retrieved on November 27, 2005, from http://www.aapc.com/pdf/SalarySrv2004.pdf

American Association of Medical Transcription (2005, July), HIPAA for MTs (Version 2.1). Retrieved on November 14, 2005, from http://www.aamt.org/scriptcontent/Downloads/delegate/packet/HipaaForMTs.doc

American Association of Medical Transcription (year unknown), Medical transcription service providers: transcription agreement checklist. Retrieved on November 11, 2005, from http://www.aamt.org/scriptcontent/Downloads/position/ChecklistTranscriptionServiceProviders.pdf

American Association of Medical Transcription (year unknown), Safeguarding protected health information (PHI): focus points for offsite transcriptionists. Retrieved on November 11, 2005, from http://www.aamt.org/scriptcontent/Downloads/position/OffsiteMTChecklist.pdf

Andrews, J. (2003). *A+ guide to software: managing, maintaining, and troubleshooting* (2nd ed., pp. 418-465). Boston: Course Technology.

ASTM International (2002). *E1902-02: Specification for Management of the Confidentiality and Security of Dictation, Transcription, and Transcribed Health Records*. West Conshohocken, PA: ASTM International.

Bureau of Labor Statistics (2005, November). National occupational employment and wage estimates November 2004: medical records and health information technicians. Retrieved on November 27, 2005, from http://www.bls.gov/oes/current/oes292071.htm

Bureau of Labor Statistics (2005, November). National occupational employment and wage estimates November 2004: medical transcriptionists. Retrieved on November 27, 2005, from http://www.bls.gov/oes/current/oes319094.htm

Bureau of Labor Statistics (2005, September). Table 1. Job-related work at home on primary job by sex, occupation, industry, race, Hispanic or Latino ethnicity, educational attainment, class of worker, and pay status, May 2004. Retrieved on November 24, 2005, from http://www.bls.gov/news.release/homey.t01.htm

Bureau of Labor Statistics (2005, September). Work at home in 2004. Retrieved November 24, 2005, from http://www.bls.gov/news.release/homey.nr0.htm

Byers, F. (2003, December 12). Government information preservation working group Retrieved November 12, 2005, from http://www.itl.nist.gov/div895/gipwog/GIPWG-Dec16.ppt#1

Centers for Medicare and Medicaid Services (2004, August). Medical privacy - national standards to protect the privacy of personal health information sample business associate contract provisions. (Originally published in FR 67 No. 157 on August 14, 2002). Retrieved on November 24, 2005 from http://www.hhs.gov/ocr/hipaa/contractprov.html

Centers for Medicare and Medicaid Services (2004, September). "HIPAA Administrative Simplification - Transactions & Code Sets." Retrieved on November 25, 2005, from http://www.cms.hhs.gov/hipaa/hipaa2/regulations/transactions/default.asp

Centers for Medicare and Medicaid Services (2004, September). The Health Insurance Portability and Accountability Act of 1996 (HIPAA). Retrieved November 12, 2005, from http://www.cms.hhs.gov/hipaa/

Centers for Medicare and Medicaid Services (2004, November). "HIPAA information series 1: Security 101 for Covered Entities Retrieved on November 25, 2005, from http://www.cms.hhs.gov/hipaa/hipaa2/education/Security%20101_Cleared.pdf

Centers for Medicare and Medicaid Services (2005, May). "HIPAA information series 2: Security Standards, Administrative Safeguards." Retrieved on November 25, 2005, from http://www.cms.hhs.gov/hipaa/hipaa2/education/HIPAA%20Security%20Series%20Administrative%20Safeguards.pdf

Centers for Medicare and Medicaid Services (2005, February). "HIPAA information series 3: Security Standards: Physical Safeguards". Retrieved on November 25, 2005, from http://www.cms.hhs.gov/hipaa/hipaa2/education/Physical%20Safeguards%20final.pdf

Centers for Medicare and Medicaid Services (2005, May). "HIPAA information series 4: Security Standards: Technical Safeguards. Retrieved on November 25, 2005, from

http://www.cms.hhs.gov/hipaa/hipaa2/education/HIPAA%20Security%20Series%20Technical%20Safeguards.pdf

Centers for Medicare and Medicaid Services (2003, May). "HIPAA information series 5: Vendor, Billing Service, Clearinghouse Readiness". Retrieved on November 25, 2005, from http://www.cms.hhs.gov/hipaa/hipaa2/education/infoserie/5-VendorBillingservice.PDF

Connor, D. (2005, November 14). Telling tales of the tape. *Network World. Retrieved on November 13, 2005, from* http://www.networkworld.com/news/2005/111405widernet.html

Department of Justice (2005, June). Scope of criminal enforcement under 42 U.S.C. § 1320d-6. Retrieved on November 26, 2005, from http://www.usdoj.gov/olc/hipaa_final.htm

Davino, M. (2004, March). Assessing privacy risk in outsourcing. *Journal of AHIMA, 75* (3), 42-46. Retrieved on November 11, 2005, from http://library.ahima.org/xpedio/groups/public/documents/ahima/pub_bok1_022546.html

Davis, N. Lemery, C. & Roberts, K. (2005, April). Identity theft and fraud – the impact on HIM operations (AHIMA practice brief). *Journa of AHIMA, 76* (4), 64A-D.

Dougherty, M. & Scichilone, R. (2002). Practice brief: establishing a telecommuting or home-based employee program (updated). *Journal of AHIMA, 73* (7), 72A-L. (1999 version originally prepared by Fletcher, D.) Retrieved November 11, 2005, from http://library.ahima.org/xpedio/groups/public/documents/ahima/pub_bok1_013767.html

Fadlalla, A. & Wickramasinghe, N. (2004). "An integrative framework for HIPAA-compliant I*IQ healthcare information system." *International Journal of Health Care Quality, 17* (2/3), p. 65. Retrieved on November 20, 2005, from http://nclive.lib.ncsu.edu:2068/pqdweb?did=670966961&sid=1&Fmt=4&clientId=15092&RQT=309&VName=PQD

Federal Register (2003, February 20). Health insurance reform: security standards. 45 CFR Parts 160, 162, and 164. *Rules and Regulation, 68* (34), 8334. Retrieved November 12, 2005, from http://63.241.27.79/providerupdate/regs/cms0049f.pdf

Federal Trade Commission (2004, June 15). Provisions of new fair and accurate credit transactions act will help reduce identity theft and help victims recover. Retrieved on November 23, 2005, from http://www.ftc.gov/opa/2004/06/factaidt.htm

Federal Trade Commission (2004, November 18). FTC issues final regulation on consumer information and records disposal. Retrieved on November 24, 2005 from http://www.ftc.gov/opa/2004/11/factadisposal.htm

Fohl, J. (2005, August). How to handle disaster recovery with Windows XP's system restore. Retrieved on November 23, 2005, from http://free-backup.info/handle-disaster-recovery-windows-xps-system-restore.html

Fohl, J. (2005, September). Alternatives to tape backup http://free-backup.info/alternatives-to-tape-backup.html

Frazier, C. (2003, April 2). The Added Edge. Retrieved on November 27, 2005, from http://www.aapc.com/other/added_edge/archive/03_0402.html

Gilbert, C. (2004, March/April). Privacy certification for business associates: marketing compliance standards for profit. *Journal of the American Association for Medical Transcription, 23* (2), 98-101.

Gostin, L. (2001, June 20). National health information privacy: regulations under the health insurance portability and accountability act. *Journal of the American Medical Association, 285* (23), 3015-3021.

Hash, J., Bowen, P., Johnson, A., Smith, C., & Steinberg, D. (2005). NIST special publication 800-66: an introductory resource guide for implementing the health insurance portability and accountability act (HIPAA) security rule. Retrieved on November 11, 2005, from http://csrc.nist.gov/publications/nistpubs/800-66/SP800-66.pdf

Health and Human Services (2003, July 18). Health Information Privacy and Civil Rights Questions & Answers: must I provide patients with access to oral information? Retrieved on November 23, 2005, from http://healthprivacy.answers.hhs.gov/cgi-bin/hipaa.cfg/php/enduser/std_adp.php?p_faqid=369&p_created=1040408957&p_sid=smndMzVh&p_lva=246&p_sp=cF9zcmNoPTEmcF9zb3J0X2J5PWRmbHQmcF9ncmlkc29ydD0mcF9yb3dfY250PTUmcF9wcm9kcz0mcF9jYXRzPTcsMCZwX3B2PSZwX2N2PTEuNzsyLnUwJnBfc2VhcmNoX3R5cGU9YW5zd2Vycy5zZWFyY2hfbmwmcF9wYWdlPTEmcF9zZWFyY2hfdGV4dD1vcmFs&p_li=&p_topview=1

Hospitals for a Healthy Environment (2003). Waste Reduction. Retrieved on November 23, 2005, from http://www.h2e-online.org/tools/waste_hipaa.htm

Hurley, B. (2004, September/October). What is ASTM, and who cares? *Journal of the American Association for Medical Transcription, 23* (5), 288-292.

ITAC (2005, October 4). Annual survey shows Americans are working from many different locations outside their employer's office. Retrieved on November 26, 2005, from http://www.workingfromanywhere.org/news/pr100405.htm

Kahles, M. (1991, April). Paper shredders: eliminating the risks. T*he CPA Journal Online.* Retrieved November 22, 2005, from http://www.nysscpa.org/cpajournal/old/10691669.htm

Krager, D. & Krager, C. (2005). *HIPAA for medical office personnel*. Clifton Park, NY: Delmar Learning.

Kuhn, R., Tracy, M. & Frankel, S. (2002, August). *NIST Special Publication 800-46: Security for Telecommuting and Broadband Communications.* Washington: U.S. Government Printing Office.

Lo, B., Dornbrand, L., & Dubler, N. (2005, April 13). HIPAA and patient care. *Journal of the American Medical Association, 66* (14), 1766-1771.

Mackey, D. (2003). *Web security for network and system administrators.* p. 307. Boston: Course Technology.

Martin, J. (2004, November 18). Online backup services: safe, simple options for backing up, plus: a lesson from Kim Novak. *PC World.* Retrieved on November 23, 2005, from http://www.pcworld.com/howto/article/0,aid,118454,00.asp

Microsoft (2005, May 25). Privacy progress. Retrieved November 22, 2005, from http://www.microsoft.com/mscorp/twc/privacy/progress.mspx

Mississippi Hospital Association (2004). Health careers center: medical billing clerk. Retrieved November 22, 2005, from http://www.mshealthcareers.com/careers/medicalbillingclerk.htm

Mississippi Hospital Association (2004). Health careers center: medical coding specialist. Retrieved November 22, 2005, from http://www.mshealthcareers.com/careers/medicalcoding.htm

Mississippi Hospital Association (2004). Health careers center: medical transcriptionist. Retrieved November 22, 2005, from http://www.mshealthcareers.com/careers/medicaltranscipt.htm

Office for Civil Rights (2003, April). What you should know about OCR HIPAA privacy rule guidance materials. Retrieved November 22, 2005, from http://www.hhs.gov/ocr/hipaa/misleadingmarketing.html

Office of Civil Rights (2003, May). Privacy brief: summary of the hipaa privacy rule. Retrieved on November 26, 2005, from http://www.hhs.gov/ocr/privacysummary.pdf

Perry, K. (2004, December 17). Practice management Q&As: HIPAA-compliant paper disposal. *Medical Economics, 81,* (24), 48.

Rhodes, H., Dennis, J. & Roach, M. (2003, April). Overseas outsourcing: the risk of doing business? *Journal of AHIMA, 75* (4), 26-31. Retrieved on November 11, 2005, from http://library.ahima.org/xpeido/groups/public/documents/ahima/pub_bok1_022641.html

Rhodes, H. & Hughes, G. (2003, April). AHIMA Practice Brief: Letters of agreement/contracts. (Originally published June 2001 in Journal of AHIMA, 72 (6)). Retrieved on November 11, 2005, from http://library.ahima.org/xpedio/groups/public/documents/ahima/pub_bok1_018254.html

Rowell, J. & Green, M. (2004). *Understanding health insurance: a guide to professional billing (7th ed).* Clifton Park, NY: Delmar Learning.

Shearer, J. (2001, April). Remote coding at home: tips for success. *Journal of AHIMA, 72* (2), 62-65.

Shniper, L. (2001). Medical transcriptionists: making medical histories. *Occupational Outlook Quarterly Online, 45* (3), 34-37. Retrieved on November 27, 2005, from http://www.bls.gov/opub/ooq/2001/fall/art06.htm

University of Arizona, Tucson (2004, March 24). Risk reduction: computer protections and prevention. Retrieved November 12, 2005, from http://web.arizona.edu/~security/RiskReduction.pdf

University of Arizona, Tucson (2004, March 24). Security basics: guide for securing your personal computer. Retrieved November 12, 2005, from http://web.arizona.edu/~security/Security.pdf

University of Texas at Austin (2004, June 3). Choosing your password. Retrieved November 12, 2005, from http://www.utexas.edu/computer/passwords/choose.html

US-CERT (2005, June 13). Home computer security. (Original work published 2002). Retrieved on November 27, 2005, from http://www.uscert.gov/reading_room/HomeComputerSecurity/

W3Schools (2005, November). Browser Statistics. Retrieved on November 28, 2005, from http://www.w3schools.com/browsers/browsers_stats.asp

WEDI - SNIP (2004, January). Business associate example: medical transcription white paper (Final version, January 2004). Retrieved November 22, 2005, from http://wedi.org/cmsUploads/pdfUpload/WhitePaper/pub/C-432_Final-BA-Transcription.pdf

WEDI SNIP (2002, August 26). Transaction compliance and certification: a white paper describing the recommended solutions for compliance testing and certification of the HIPAA transactions version 3.0. Retrieved on November 27, 2005, from http://www.wedi.org/snip/public/articles/testing_whitepaper082602.pdf

Whitehead, A. (2005, September). Basic data recovery. Retrieved on November 23, 2005, from http://free-backup.info/basic-data-recovery.html

Whitehead, A. (2005, September). What is an online backup? Retrieved on November 23, 2005, from http://free-backup.info/what-is-an-online-backup.html

Whitman, M. & Mattord, H. (2004). *Management of information security*, p. 307. Boston: Course Technology.